

Journal of Cybersecurity Education, Research and Practice

Volume 2017 | Number 2

Article 1

December 2017

From the Editors

Herbert J. Mattord

Kennesaw State University, hmattord@kennesaw.edu

Michael E. Whitman

Kennesaw State University, mwhitman@kennesaw.edu

Carole L. Hollingsworth

Kennesaw State University, chollin2@kennesaw.edu

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/jcerp>



Part of the [Information Security Commons](#), [Management Information Systems Commons](#), and the [Technology and Innovation Commons](#)

Recommended Citation

Mattord, Herbert J.; Whitman, Michael E.; and Hollingsworth, Carole L. (2017) "From the Editors," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2017 : No. 2 , Article 1.

Available at: <https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss2/1>

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

From the Editors

Keywords

Editorial, researcher/educator responsibility, curriculum

FROM THE EDITORS

Welcome to the Winter 2017 issue of the Journal of Cybersecurity Education, Research, and Practice (JCERP). On behalf of the editorial team, we thank you for taking the time to read this issue and strongly encourage you to consider submitting an article for consideration in an upcoming edition.

For this issue's editorial, we share some thoughts on our perception of the responsibility researchers and educators have to support the practice of cybersecurity in industry and government.

Some of us that teach and write for the cybersecurity classroom come from a background that includes working in the field of security where we have been responsible for securing the information assets of organizations. Others on the academic side of cybersecurity have not had those practical experiences and work to prepare students to work in the field without the benefits and insights that experience provides. Regardless of our background, we all work toward the key outcome of our efforts — to deliver well-prepared graduates to the workforce. But, what else is expected?

First, the curriculum used to prepare students must be current and aligned with the needs and expectations of the organizations who will employ them. Each cybersecurity program should make an ongoing and sustained effort to align their curriculum with both the national and international needs articulated in guidance documents. Those sources of guidance include the NIST NICE Cybersecurity Workforce Framework, the Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity from the ACM/IEEE/AIS/IFIP Joint Task Force on Cybersecurity Education, or other formal guidance from one of many national and international authorities.

While alignment to international and national needs is important, it is equally important that programs of study meet the needs of local stakeholders. Many institutions with programs of study in cybersecurity rely on local advisory boards to offer specific feedback on local needs to incorporate into the curriculum.

A second consideration should be to make an effort to provide students in academic programs with practical skills with wide applicability. These skills are augmented with on-the-job experiences provided through experiential learning activities such as co-operative studies and internships whenever possible.

Finally, academic faculty engaged in research activities should make an effort to keep some degree of focus on practicality. Selecting topics of interest to the practice community as part of that effort, while ensuring every project includes some aspect of application of the results of research to the benefit of the practice community.

Each of us involved in the academic process should make an effort to improve the cybersecurity workforce and the effectiveness of those already working in the field. There are a number of ways we can accomplish this as we combine research with teaching and service. What's important is to make a concerted effort to maximize our work products – in terms of students, articles, and service contributions – for the benefits of our stakeholders.

The mission of JCERP is to be the premier outlet for high-quality information security and cybersecurity related articles of interest to teaching faculty and students.

The JCERP Editorial Team:

Herbert J. Mattord, Ph.D., CISM, CISSP, Co-Editor in Chief
Michael E. Whitman, Ph.D., CISM, CISSP, Co-Editor in Chief
Carole Hollingsworth, DBA, Senior Editor
Kennesaw State University, GA, USA
infosec@kennesaw.edu

For a complete listing of the Associate Editors, or to submit a manuscript please visit the JCERP Web site at digitalcommons.kennesaw.edu/jcerp/